修 士 論 文 の 和 文 要 旨

研究科・専攻	大学院 情報システム学研究科 情報ネットワークシステム学専攻 博士前期課程		
氏　　名	川島　千種	学籍番号	0852009
論 文 題 目	秘密分散法を用いた相互匿名通信 (Mutually Anonymous Communication Using Secret Sharing Schemes)		

要　　旨

近年、Peer-to-Peer通信が一般的になってきたことから、ユーザのプライバシー保護のために匿名性の実現が求められている。パケット通信ではIPパケットのヘッダ部に送信元のアドレスが記載されるため、ユーザに匿名性を与えるためには特別なルーティング技術が必要となる。

1997年にSyversonらが提案したonion routingは、送信先を含め他のピアから送信者のIPアドレスを秘匿するルーティング法である。しかし、この方式ではIPアドレスの秘匿に公開鍵暗号を利用しており、事前に信頼できる第三者機関(PKI等)が鍵を配送する必要がある。これに伴い、鍵配送や鍵更新等の問題が生じるため、システムの信頼性や拡張性を損なう原因となっている。この問題を解決するため、2005年にKattiらはPKIを必要としない匿名通信法であるinformation slicingを提案した。これは暗号化を行う代わりにメッセージの分散情報を並列パスに沿って送信することで、匿名性を実現するものである。　また、メッセージ分散の際に冗長性を持たせることで、パス上のピアが欠落した場合にも通信に耐久性を持たせることができる。

上記の二方式は送信者から受信者に向かって一方向の匿名性を実現する技術だが、2005年にHanらによって提案された Secret-sharing-based Mutual Anonymous Protocol(SSMP) は送信者と受信者の相互匿名を実現するプロトコルである。SSMPはonion routingの技術を用いて構成されているため、上記のような公開鍵暗号を用いることの問題点がある。

そこで本論文では、SSMPをonion routingではなくinformation slicingを用いて構成する相互匿名通信プロトコルを提案する。評価ではinformation slicingとonion routingのデータ伝送の信頼性の比較を行い、双方が等しいリンク数で通信を行った場合にもinformation slicingを用いた場合の方が信頼性が上がることを示した。また、システム内に送信者を特定しようとするピアが存在する場合の匿名性に関する評価も行い、攻撃の成功確率の観点から、information slicingの方がonion routingよりもより高い匿名性を持つことを示した。